CompTIA Cybersecurity Analyst (CySA+)
Certification Exam Objectives

EXAM NUMBER: CS0-002
About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA Cybersecurity Analyst (CySA+) CS0-002 certification exam. With the end goal of proactively defending and continuously improving the security of an organization, CySA+ will verify the successful candidate has the knowledge and skills required to:

• Leverage intelligence and threat detection techniques
• Analyze and interpret data
• Identify and address vulnerabilities
• Suggest preventative measures
• Effectively respond to and recover from incidents

This is equivalent to 4 years of hands-on experience in a technical cybersecurity job role.

These content examples are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

CompTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse or condone utilizing any content provided by unauthorized third-party training sites (aka “brain dumps”). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA’s exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka “brain dumps”), he/she should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current and the security of the questions is protected. When necessary, we will publish updated exams based on testing exam objectives. Please know that all related exam preparation materials will still be valid.
TEST DETAILS
Required exam CS0-002
Number of questions Minimum of 85
Type of questions Multiple choice and performance-based
Length of test 165 minutes
Recommended experience
• 4 years of hands-on experience in a technical cybersecurity job role
• Security+ and Network+, or equivalent knowledge and experience
Passing score 750

EXAM OBJECTIVES (DOMAINS)
The table below lists the domains measured by this examination and the extent to which they are represented.

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>PERCENTAGE OF EXAMINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Threat and Vulnerability Management</td>
<td>22%</td>
</tr>
<tr>
<td>2.0 Software and Systems Security</td>
<td>18%</td>
</tr>
<tr>
<td>3.0 Security Operations and Monitoring</td>
<td>25%</td>
</tr>
<tr>
<td>4.0 Incident Response</td>
<td>22%</td>
</tr>
<tr>
<td>5.0 Compliance and Assessment</td>
<td>13%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
1.0 Threat and Vulnerability Management

1.1 Explain the importance of threat data and intelligence.

- **Intelligence sources**
  - Open-source intelligence
  - Proprietary/closed-source intelligence
  - Timeliness
  - Relevancy
  - Accuracy
- **Confidence levels**
- **Indicator management**
  - Structured Threat Information eXpression (STIX)
  - Trusted Automated eXchange of Indicator Information (TAXII)
  - OpenIOC
- **Threat classification**
  - Known threat vs. unknown threat
  - Zero-day
  - Advanced persistent threat
- **Threat actors**
  - Nation-state
  - Hacktivist
  - Organized crime
  - Insider threat
    - Intentional
    - Unintentional
- **Intelligence cycle**
  - Requirements
  - Collection
  - Analysis
  - Dissemination
  - Feedback
- **Commodity malware**
- **Information sharing and analysis communities**
  - Healthcare
  - Financial
  - Aviation
  - Government
  - Critical infrastructure

1.2 Given a scenario, utilize threat intelligence to support organizational security.

- **Attack frameworks**
  - MITRE ATT&CK
  - The Diamond Model of Intrusion Analysis
  - Kill chain
- **Threat research**
  - Reputational
  - Behavioral
  - Indicator of compromise (IOC)
- **Threat modeling methodologies**
  - Adversary capability
  - Total attack surface
  - Attack vector
  - Impact
  - Likelihood
  - Common vulnerability scoring system (CVSS)
- **Threat intelligence sharing with supported functions**
  - Incident response
  - Vulnerability management
  - Risk management
  - Security engineering
  - Detection and monitoring
### 1.0 Threat and Vulnerability Management

#### 1.3 Given a scenario, perform vulnerability management activities.

<table>
<thead>
<tr>
<th>Category</th>
<th>Activities</th>
</tr>
</thead>
</table>
| **Vulnerability identification** | - Asset criticality  
- Active vs. passive scanning  
- Mapping/enumeration |
| **Validation**         | - True positive  
- False positive  
- True negative  
- False negative |
| **Remediation/mitigation** | - Configuration baseline  
- Patching  
- Hardening  
- Compensating controls |
| **Scanning parameters and criteria** | - Risks associated with scanning activities  
- Vulnerability feed  
- Scope  
- Credentialized vs. non-credentialized  
- Server-based vs. agent-based  
- Internal vs. external |
| **Remediation/mitigation** | - Special considerations  
- Types of data  
- Technical constraints  
- Workflow |
| **Risk acceptance**    | - Verification of mitigation  
- True positive  
- False positive  
- True negative  
- False negative |
| **Remediation/mitigation** | - Configuration baseline  
- Patching  
- Hardening  
- Compensating controls |
| **Scanning parameters and criteria** | - Risks associated with scanning activities  
- Vulnerability feed  
- Scope  
- Credentialized vs. non-credentialized  
- Server-based vs. agent-based  
- Internal vs. external |
| **Remediation/mitigation** | - Special considerations  
- Types of data  
- Technical constraints  
- Workflow |
| **Risk acceptance**    | - Verification of mitigation  
- True positive  
- False positive  
- True negative  
- False negative |
| **Remediation/mitigation** | - Configuration baseline  
- Patching  
- Hardening  
- Compensating controls |

#### 1.4 Given a scenario, analyze the output from common vulnerability assessment tools.

<table>
<thead>
<tr>
<th>Tool Type</th>
<th>Tools</th>
</tr>
</thead>
</table>
| Web application scanner       | - OWASP Zed Attack Proxy (ZAP)  
- Burp suite  
- Nikto  
- Arachni |
| Infrastructure vulnerability scanner | - Nessus  
- OpenVAS  
- Qualys |
| Software assessment tools and techniques | - Static analysis  
- Dynamic analysis  
- Reverse engineering  
- Fuzzing |
| Enumeration                    | - Nmap  
- hping  
- Active vs. passive  
- Responder |
| Wireless assessment tools      | - Aircrack-ng  
- Reaver  
- oclHashcat |
| Cloud infrastructure assessment tools | - ScoutSuite  
- Prowler  
- Pacu |

#### 1.5 Explain the threats and vulnerabilities associated with specialized technology.

<table>
<thead>
<tr>
<th>Technology Type</th>
<th>Technologies</th>
</tr>
</thead>
</table>
| Mobile                              | - Physical access control  
- Building automation systems  
- Vehicles and drones  
- Workflow and process automation systems  
- Incident command system (ICS) |
| Internet of Things (IoT)            | - CAN bus  
- Modbus |
| Embedded                            | - CAN bus  
- Modbus |
| Real-time operating system (RTOS)   | - CAN bus  
- Modbus |
| System-on-Chip (SoC)                | - CAN bus  
- Modbus |
| Field programmable gate array (FPGA)| - CAN bus  
- Modbus |
| Supervisory control and data acquisition (SCADA) | - CAN bus  
- Modbus |
1.6 Explain the threats and vulnerabilities associated with operating in the cloud.

- **Cloud service models**
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)
- **Cloud deployment models**
  - Public
  - Private
  - Community
  - Hybrid
- **Function as a Service (FaaS)/ serverless architecture**
- **Infrastructure as code (IaC)**
- **Insecure application programming interface (API)**
- **Improper key management**
- **Unprotected storage**
- **Logging and monitoring**
  - Insufficient logging and monitoring
  - Inability to access

1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities.

- **Attack types**
  - Extensible markup language (XML) attack
  - Structured query language (SQL) injection
  - Overflow attack
    - Buffer
    - Integer
    - Heap
  - Remote code execution
  - Directory traversal
  - Privilege escalation
- **Vulnerabilities**
  - Improper error handling
  - Dereferencing
  - Insecure object reference
  - Race condition
  - Broken authentication
  - Sensitive data exposure
  - Insecure components
  - Insufficient logging and monitoring
  - Weak or default configurations
  - Use of insecure functions
  - strcpy
## 2.0 Software and Systems Security

### 2.1 Given a scenario, apply security solutions for infrastructure management.

<table>
<thead>
<tr>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cloud vs. on-premises</strong></td>
</tr>
<tr>
<td><strong>Asset management</strong></td>
</tr>
<tr>
<td>- Asset tagging</td>
</tr>
<tr>
<td><strong>Segmentation</strong></td>
</tr>
<tr>
<td>- Physical</td>
</tr>
<tr>
<td>- Virtual</td>
</tr>
<tr>
<td>- Jumpbox</td>
</tr>
<tr>
<td>- System isolation</td>
</tr>
<tr>
<td>- Air gap</td>
</tr>
<tr>
<td><strong>Network architecture</strong></td>
</tr>
<tr>
<td>- Physical</td>
</tr>
<tr>
<td>- Software-defined</td>
</tr>
<tr>
<td><strong>Change management</strong></td>
</tr>
<tr>
<td>- Virtual private cloud (VPC)</td>
</tr>
<tr>
<td>- Virtual private network (VPN)</td>
</tr>
<tr>
<td>- Serverless</td>
</tr>
<tr>
<td><strong>Virtualization</strong></td>
</tr>
<tr>
<td>- Virtual desktop infrastructure (VDI)</td>
</tr>
<tr>
<td><strong>Containerization</strong></td>
</tr>
<tr>
<td><strong>Identity and access management</strong></td>
</tr>
<tr>
<td>- Privilege management</td>
</tr>
<tr>
<td>- Multifactor authentication (MFA)</td>
</tr>
<tr>
<td>- Single sign-on (SSO)</td>
</tr>
<tr>
<td>- Federation</td>
</tr>
<tr>
<td><strong>Change management</strong></td>
</tr>
<tr>
<td><strong>Virtualization</strong></td>
</tr>
<tr>
<td>- Virtual desktop infrastructure (VDI)</td>
</tr>
<tr>
<td><strong>Containerization</strong></td>
</tr>
<tr>
<td><strong>Identity and access management</strong></td>
</tr>
<tr>
<td>- Privilege management</td>
</tr>
<tr>
<td>- Multifactor authentication (MFA)</td>
</tr>
<tr>
<td>- Single sign-on (SSO)</td>
</tr>
<tr>
<td>- Federation</td>
</tr>
<tr>
<td><strong>Role-based</strong></td>
</tr>
<tr>
<td><strong>Attribute-based</strong></td>
</tr>
<tr>
<td><strong>Mandatory</strong></td>
</tr>
<tr>
<td><strong>Manual review</strong></td>
</tr>
<tr>
<td><strong>Cloud access security broker (CASB)</strong></td>
</tr>
<tr>
<td><strong>Honeypot</strong></td>
</tr>
<tr>
<td><strong>Monitoring and logging</strong></td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
</tr>
<tr>
<td><strong>Certificate management</strong></td>
</tr>
<tr>
<td><strong>Active defense</strong></td>
</tr>
</tbody>
</table>

### 2.2 Explain software assurance best practices.

<table>
<thead>
<tr>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Platforms</strong></td>
</tr>
<tr>
<td>- Mobile</td>
</tr>
<tr>
<td>- Web application</td>
</tr>
<tr>
<td>- Client/server</td>
</tr>
<tr>
<td>- Embedded</td>
</tr>
<tr>
<td>- System-on-chip (SoC)</td>
</tr>
<tr>
<td>- Firmware</td>
</tr>
<tr>
<td><strong>Software development life cycle (SDLC) integration</strong></td>
</tr>
<tr>
<td><strong>DevSecOps</strong></td>
</tr>
<tr>
<td><strong>Software assessment methods</strong></td>
</tr>
<tr>
<td><strong>User acceptance testing</strong></td>
</tr>
<tr>
<td><strong>Stress test application</strong></td>
</tr>
<tr>
<td><strong>Security regression testing</strong></td>
</tr>
<tr>
<td><strong>Code review</strong></td>
</tr>
<tr>
<td><strong>Static analysis tools</strong></td>
</tr>
<tr>
<td><strong>Dynamic analysis tools</strong></td>
</tr>
<tr>
<td><strong>Formal methods for verification of critical software</strong></td>
</tr>
<tr>
<td><strong>Service-oriented architecture</strong></td>
</tr>
<tr>
<td>- Security Assertions</td>
</tr>
<tr>
<td>- Markup Language (SAML)</td>
</tr>
<tr>
<td>- Simple Object Access Protocol (SOAP)</td>
</tr>
<tr>
<td>- Representational State Transfer (REST)</td>
</tr>
<tr>
<td>- Microservices</td>
</tr>
</tbody>
</table>

### 2.3 Explain hardware assurance best practices.

<table>
<thead>
<tr>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware root of trust</strong></td>
</tr>
<tr>
<td>- Trusted platform module (TPM)</td>
</tr>
<tr>
<td>- Hardware security module (HSM)</td>
</tr>
<tr>
<td><strong>eFuse</strong></td>
</tr>
<tr>
<td><strong>Unified Extensible Firmware Interface (UEFI)</strong></td>
</tr>
<tr>
<td><strong>Trusted foundry</strong></td>
</tr>
<tr>
<td><strong>Secure processing</strong></td>
</tr>
<tr>
<td>- Trusted execution</td>
</tr>
<tr>
<td>- Secure enclave</td>
</tr>
<tr>
<td>- Processor security extensions</td>
</tr>
<tr>
<td>- Atomic execution</td>
</tr>
<tr>
<td><strong>Anti-tamper</strong></td>
</tr>
<tr>
<td><strong>Self-encrypting drive</strong></td>
</tr>
<tr>
<td><strong>Trusted firmware updates</strong></td>
</tr>
<tr>
<td><strong>Measured boot and attestation</strong></td>
</tr>
<tr>
<td><strong>Bus encryption</strong></td>
</tr>
</tbody>
</table>

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives 2.0 (Exam Number: CS0-002)
3.0 Security Operations and Monitoring

3.1 Given a scenario, analyze data as part of security monitoring activities.

- **Heuristics**
- **Trend analysis**
- **Endpoint**
  - Malware
  - Reverse engineering
  - Memory
  - System and application behavior
    - Known-good behavior
    - Anomalous behavior
    - Exploit techniques
  - File system
  - User and entity behavior analytics (UEBA)
- **Network**
  - Uniform Resource Locator (URL) and domain name system (DNS) analysis
  - Dynamically generated algorithms
  - Flow analysis
  - Packet and protocol analysis
  - Malware
- **Log review**
  - Event logs
  - Syslog
  - Firewall logs
  - Web application firewall (WAF)
  - Proxy
  - Intrusion detection system (IDS)/Intrusion prevention system (IPS)
- **Impact analysis**
  - Organization impact vs. localized impact
  - Immediate vs. total
- **Security information and event management (SIEM) review**
  - Rule writing
  - Known-bad Internet protocol (IP)
  - Dashboard
- **Query writing**
  - String search
  - Script
  - Piping
- **E-mail analysis**
  - Malicious payload
  - Domain Keys Identified Mail (DKIM)
  - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
  - Sender Policy Framework (SPF)
  - Phishing
  - Forwarding
  - Digital signature
  - E-mail signature block
  - Embedded links
  - Impersonation
  - Header

3.2 Given a scenario, implement configuration changes to existing controls to improve security.

- **Permissions**
- **Whitelisting**
- **Blacklisting**
- **Firewall**
- **Intrusion prevention system (IPS) rules**
- **Data loss prevention (DLP)**
- **Endpoint detection and response (EDR)**
- **Network access control (NAC)**
- **Sinkholing**
- **Malware signatures**
  - Development/rule writing
- **Sandboxing**
- **Port security**
3.3 Explain the importance of proactive threat hunting.

- Establishing a hypothesis
- Profiling threat actors and activities
- Threat hunting tactics
  - Executable process analysis
- Reducing the attack surface area
- Bundling critical assets
- Attack vectors
- Integrated intelligence
- Improving detection capabilities

3.4 Compare and contrast automation concepts and technologies.

- Workflow orchestration
- Scripting
- Application programming interface (API) integration
- Automated malware signature creation
- Data enrichment
- Threat feed combination
- Machine learning
- Use of automation protocols and standards
  - Security Content Automation Protocol (SCAP)
- Continuous integration
- Continuous deployment/delivery
4.0 Incident Response

4.1 Explain the importance of the incident response process.

- Communication plan
  - Limiting communication to trusted parties
  - Disclosing based on regulatory/legislative requirements
  - Preventing inadvertent release of information
  - Using a secure method of communication
  - Reporting requirements

- Response coordination with relevant entities
  - Legal
  - Human resources
  - Public relations
  - Internal and external
  - Law enforcement
  - Senior leadership
  - Regulatory bodies

- Factors contributing to data criticality
  - Personally identifiable information (PII)
  - Personal health information (PHI)
  - Special protected information (SPI)
  - High value asset
  - Financial information
  - Intellectual property
  - Corporate information

4.2 Given a scenario, apply the appropriate incident response procedure.

- Preparation
  - Training
  - Testing
  - Documentation of procedures

- Detection and analysis
  - Characteristics contributing to severity level classification
  - Downtime
  - Recovery time
  - Data integrity
  - Economic
  - System process criticality
  - Reverse engineering
  - Data correlation

- Containment
  - Segmentation
  - Isolation

- Eradication and recovery
  - Vulnerability mitigation
  - Sanitization
  - Reconstruction/reimaging
  - Secure disposal
  - Patching
  - Restoration of permissions
  - Reconstitution of resources
  - Restoration of capabilities and services

- Verification of logging/communication to security monitoring

- Post-incident activities
  - Evidence retention
  - Lessons learned report
  - Change control process
  - Incident response plan update
  - Incident summary report
  - Indicator of compromise (IOC) generation
  - Monitoring
4.0 Incident Response

4.3 Given an incident, analyze potential indicators of compromise.

• Network-related
  - Bandwidth consumption
  - Beaconing
  - Irregular peer-to-peer communication
  - Rogue device on the network
  - Scan/sweep
  - Unusual traffic spike
  - Common protocol over non-standard port

• Host-related
  - Processor consumption
  - Memory consumption
  - Drive capacity consumption
  - Unauthorized software
  - Malicious process
  - Unauthorized change
  - Unauthorized privilege
  - Data exfiltration
  - Abnormal OS process behavior
  - File system change or anomaly
  - Registry change or anomaly
  - Unauthorized scheduled task

• Application-related
  - Anomalous activity
  - Introduction of new accounts
  - Unexpected output
  - Unexpected outbound communication
  - Service interruption
  - Application log

4.4 Given a scenario, utilize basic digital forensics techniques.

• Network
  - Wireshark
  - tcpdump

• Endpoint
  - Disk
  - Memory

• Mobile
• Cloud

• Virtualization
• Legal hold
• Procedures
• Hashing
  - Changes to binaries
• Carving
• Data acquisition
5.0 Compliance and Assessment

5.1 Understand the importance of data privacy and protection.

- Privacy vs. security
  - Legal requirements
  - Data sovereignty
  - Data minimization
  - Purpose limitation
  - Non-disclosure agreement (NDA)
- Non-technical controls
  - Classification
  - Ownership
  - Retention
  - Data types
  - Retention standards
  - Confidentiality
  - Data masking
  - Deidentification
  - Tokenization
  - Digital rights management (DRM)
  - Watermarking
  - Geographic access requirements
  - Access controls
- Technical controls
  - Encryption
  - Data loss prevention (DLP)

5.2 Given a scenario, apply security concepts in support of organizational risk mitigation.

- Business impact analysis
- Risk identification process
- Risk calculation
  - Probability
  - Magnitude
- Communication of risk factors
- Risk prioritization
  - Security controls
  - Engineering tradeoffs
- Systems assessment
- Documented compensating controls
- Training and exercises
  - Red team
  - Blue team
  - White team
  - Tabletop exercise
- Supply chain assessment
  - Vendor due diligence
  - Hardware source authenticity

5.3 Explain the importance of frameworks, policies, procedures, and controls.

- Frameworks
  - Risk-based
  - Prescriptive
- Policies and procedures
  - Code of conduct/ethics
  - Acceptable use policy (AUP)
  - Password policy
  - Data ownership
- Data retention
- Account management
- Continuous monitoring
- Work product retention
- Control types
  - Managerial
  - Operational
  - Technical
- Preventative
- Detective
- Responsive
- Corrective
- Audits and assessments
  - Regulatory
  - Compliance

Understand the importance of data privacy and protection.

Given a scenario, apply security concepts in support of organizational risk mitigation.

Explain the importance of frameworks, policies, procedures, and controls.
CompTIA Cybersecurity Analyst (CySA+) Acronym List

The following is a list of acronyms that appear on the CompTIA CySA+ exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as a part of a comprehensive exam preparation program.

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>ATT&amp;CK</td>
<td>Adversarial Tactics, Techniques, and Common Knowledge</td>
</tr>
<tr>
<td>AUP</td>
<td>Acceptable Use Policy</td>
</tr>
<tr>
<td>BEC</td>
<td>Business Email Compromise</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</td>
</tr>
<tr>
<td>CAN</td>
<td>Controller Area Network</td>
</tr>
<tr>
<td>CASB</td>
<td>Cloud Access Security Broker</td>
</tr>
<tr>
<td>CIS</td>
<td>Center for Internet Security</td>
</tr>
<tr>
<td>COBIT</td>
<td>Control Objectives for Information and Related Technology</td>
</tr>
<tr>
<td>CRM</td>
<td>Customer Relations Management</td>
</tr>
<tr>
<td>CVSS</td>
<td>Common Vulnerability Scoring System</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DGA</td>
<td>Domain Generation Algorithm</td>
</tr>
<tr>
<td>DKIM</td>
<td>Domain Keys Identified Mail</td>
</tr>
<tr>
<td>DLP</td>
<td>Data Loss Prevention</td>
</tr>
<tr>
<td>DMARC</td>
<td>Domain-based Message Authentication, Reporting, and Conformance</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DOM</td>
<td>Document Object Model</td>
</tr>
<tr>
<td>DRM</td>
<td>Digital Rights Management</td>
</tr>
<tr>
<td>EDR</td>
<td>Endpoint Detection and Response</td>
</tr>
<tr>
<td>ELK</td>
<td>Elasticsearch, Logstash, Kibana</td>
</tr>
<tr>
<td>Faas</td>
<td>Function as a Service</td>
</tr>
<tr>
<td>FGPA</td>
<td>Field-programmable Gate Array</td>
</tr>
<tr>
<td>FTK</td>
<td>Forensic Toolkit</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>HIDS</td>
<td>Host Intrusion Detection System</td>
</tr>
<tr>
<td>HIPS</td>
<td>Host-based Intrusion Prevention System</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Security Module</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>IaC</td>
<td>Infrastructure as Code</td>
</tr>
<tr>
<td>ICS</td>
<td>Incident Command System</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IMAP</td>
<td>Internet Message Access Protocol</td>
</tr>
<tr>
<td>IOC</td>
<td>Indicator of Compromise</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ITIL</td>
<td>Information Technology Infrastructure Library</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>MaaS</td>
<td>Monitoring as a Service</td>
</tr>
<tr>
<td>MAC</td>
<td>Mandatory Access Control</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5</td>
</tr>
<tr>
<td>MFA</td>
<td>Multifactor Authentication</td>
</tr>
<tr>
<td>MOA</td>
<td>Memorandum of Agreement</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>MRTG</td>
<td>Multi Router Traffic Grapher</td>
</tr>
<tr>
<td>NAC</td>
<td>Network Access Control</td>
</tr>
<tr>
<td>NDA</td>
<td>Non-disclosure Agreement</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</td>
</tr>
<tr>
<td>NIDS</td>
<td>Network Intrusion Detection Systems</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>OSSIM</td>
<td>Open Source Security Information Management</td>
</tr>
<tr>
<td>OWASP</td>
<td>Open Web Application Security Project</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>PAM</td>
<td>Pluggable Authentication Module</td>
</tr>
<tr>
<td>PCI</td>
<td>Payment Card Industry</td>
</tr>
<tr>
<td>PHI</td>
<td>Personal Health Information</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-in User Service</td>
</tr>
<tr>
<td>REST</td>
<td>Representational State Transfer</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>RTOS</td>
<td>Real-time Operating System</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertions Markup Language</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SCAP</td>
<td>Security Content Automation Protocol</td>
</tr>
<tr>
<td>SDLC</td>
<td>Software Development Life Cycle</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>SOC</td>
<td>Security Operations Center</td>
</tr>
<tr>
<td>SoC</td>
<td>System on Chip</td>
</tr>
<tr>
<td>SPF</td>
<td>Sender Policy Framework</td>
</tr>
<tr>
<td>SPI</td>
<td>Special Protected Information</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign-on</td>
</tr>
<tr>
<td>STIX</td>
<td>Structured Threat Information eXpression</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller</td>
</tr>
<tr>
<td></td>
<td>Access Control System Plus</td>
</tr>
<tr>
<td>TAXII</td>
<td>Trusted Automated eXchange of Intelligence</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>UEBA</td>
<td>User and Entity Behavior Analytics</td>
</tr>
<tr>
<td>UEFI</td>
<td>Unified Extensible Firmware Interface</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>VDI</td>
<td>Virtual Desktop Infrastructure</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VPC</td>
<td>Virtual Private Cloud</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WAF</td>
<td>Web Application Firewall</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
<tr>
<td>ZAP</td>
<td>Zed Attack Proxy</td>
</tr>
</tbody>
</table>
CySA+ Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the CySA+ exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The bulleted lists below each topic are samples and are not exhaustive.

**IT HARDWARE**
- Workstation (or laptop) with ability to run VM
- Managed switch
- Firewall
- Mobile phones
- VoIP Phone
- WAP
- IDS/IPS
- IoT Devices
- Servers

**SOFTWARE**
- VM images for attack targets
- Windows Server
- Windows Client
  - Commando VM
- Linux
  - Kali
  - ParrotOS
  - Security Onion
- Chrome OS
- UTM Appliance
- pfSense
- Metasploitable
- Access to cloud instances
  - Azure
  - AWS
  - GCP
  - SIEM
  - Greylog
  - ELK
  - Splunk
  - Vulnerability scanner
    - OpenVAS
    - Nessus

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the CySA+ exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The bulleted lists below each topic are samples and are not exhaustive.